

-2-

IN THE CLAIMS

Amended claims follow. Insertions are underlined, while deletions are struck out. The status of each claim is included prior to each heading.

1. (Currently Amended) A method of minimizing the duration of a risk-assessment scan, comprising:
  - a) selecting a plurality of risk-assessment modules each including vulnerability checks associated with a risk-assessment scan, and requiring communication via at least one predetermined port;
  - b) determining a first set of ports required for communicating with network components subject to the risk-assessment modules associated with the risk-assessment scan;
  - c) executing a port scan of only the first set of ports associated with the selected risk-assessment modules, for reducing the number of ports scanned during the port scan, wherein latency is reduced since a port scan involving 65,536 ports is avoided;
  - d) determining a second set of ports based on the port scan, the second set of ports being unavailable for communicating with the network components subject to the risk-assessment modules associated with the risk-assessment scan; and
  - e) disabling the risk-assessment modules associated with the second set of ports to minimize the duration of the risk-assessment scan;
  - f) storing a third set of ports including the first set of ports and excluding the second set of ports; and
  - g) comparing the port associated with each risk-assessment module with the stored third set of ports;
  - h) wherein the risk-assessment module is disabled if the port associated with the risk-assessment module does not match at least one port of the stored third set of ports.
2. (Original) The method as recited in claim 1, wherein a plurality of the risk-assessment modules each have the same port associated therewith, and redundancy in the first set of ports is removed prior to executing the port scan.

-3-

3. (Original) The method as recited in claim 1, wherein the risk-assessment modules are user-specified.
4. (Cancelled)
5. (Cancelled)
6. (Currently Amended) The method as recited in claim [5]1, and further comprising performing the vulnerability checks of the risk-assessment module if the port associated with the risk-assessment module matches at least one port of the stored third set of ports.
7. (Cancelled)
8. (Currently Amended) A computer program product embodied on a computer readable medium for minimizing the duration of a risk-assessment scan, comprising:
  - a) computer code for selecting a plurality of risk-assessment modules each including vulnerability checks associated with a risk-assessment scan, and requiring communication via at least one predetermined port;
  - b) computer code for determining a first set of ports required for communicating with network components subject to the risk-assessment modules associated with the risk-assessment scan;
  - c) computer code for executing a port scan of the first set of ports associated with the selected risk-assessment modules, for reducing the number of ports scanned during the port scan, wherein latency is reduced since a port scan involving 65,536 ports is avoided;
  - d) computer code for determining a second set of ports based on the port scan, the second set of ports being unavailable for communicating with the network components subject to the risk-assessment modules associated with the risk-assessment scan; and
  - e) computer code for disabling the risk-assessment modules associated with the second set of ports to minimize the duration of the risk-assessment scan;

-4-

- f) computer code for storing a third set of ports including the first set of ports and excluding the second set of ports; and
  - g) computer code for comparing the port associated with each risk-assessment module with the stored third set of ports;
  - h) wherein the risk-assessment module is disabled if the port associated with the risk-assessment module does not match at least one port of the stored third set of ports.
9. (Original) The computer program product as recited in claim 8, wherein a plurality of the risk-assessment modules each have the same port associated therewith, and redundancy in the first set of ports is removed prior to executing the port scan.
10. (Original) The computer program product as recited in claim 8, wherein the risk-assessment modules are user-specified.
11. (Cancelled)
12. (Cancelled)
13. (Currently Amended) The computer program product as recited in claim [12]8, and further comprising computer code for performing the vulnerability checks of the risk-assessment module if the port associated with the risk-assessment module matches at least one port of the stored third set of ports.
14. (Cancelled)
15. (Currently Amended) A system for minimizing the duration of a risk-assessment scan, comprising:
- a) logic for selecting a plurality of risk-assessment modules each including vulnerability checks associated with a risk-assessment scan, and requiring communication via at least one predetermined port;
  - b) logic for determining a first set of ports required for communicating with network components subject to the risk-assessment modules associated with the risk-assessment scan;

-5-

- c) logic for executing a port scan of only the first set of ports associated with the selected risk-assessment modules, for reducing the number of ports scanned during the port scan, wherein latency is reduced since a port scan involving 65,536 ports is avoided;
  - d) logic for determining a second set of ports based on the port scan, the second set of ports being unavailable for communicating with the network components subject to the risk-assessment modules associated with the risk-assessment scan; and
  - e) logic for disabling the risk-assessment modules associated with the second set of ports to minimize the duration of the risk-assessment scan;
  - f) logic for storing a third set of ports including the first set of ports and excluding the second set of ports; and
  - g) logic for comparing the port associated with each risk-assessment module with the stored third set of ports;
  - h) wherein the risk-assessment module is disabled if the port associated with the risk-assessment module does not match at least one port of the stored third set of ports.
16. (Original) The system as recited in claim 15, wherein a plurality of the risk-assessment modules each have the same port associated therewith, and redundancy in the first set of ports is removed prior to executing the port scan.
17. (Original) The system as recited in claim 15, wherein the risk-assessment modules are user-specified.
18. (Cancelled)
19. (Cancelled)
20. (Currently Amended) The system as recited in claim [19]15, and further comprising logic for performing the vulnerability checks of the risk-assessment module if the port associated with the risk-assessment module matches at least one port of the stored third set of ports.
21. (Cancelled)

-6-

22. (Previously Presented) A method of minimizing the duration of a risk-assessment scan, comprising:
- a) selecting a plurality of risk-assessment modules for execution during a risk-assessment scan, the risk-assessment modules each including vulnerability checks, and requiring communication via at least one predetermined port;
  - b) determining a set of ports for communicating with a select number of network components;
  - c) executing a port scan of only the set of ports associated with the selected risk-assessment modules and the network components, for reducing the number of ports scanned during the port scan, wherein latency is reduced since a port scan involving 65,536 ports is avoided;
  - d) modifying the set of ports based on the port scan, the set of ports being modified to include only ports available for communicating with the network components;
  - e) comparing the port associated with each selected risk-assessment module with the modified set of ports; and
  - f) conditionally disabling the execution of the risk-assessment modules based on the comparison to minimize the duration of the risk-assessment scan.
23. (Previously Presented) A computer program product embodied on a computer readable medium for minimizing the duration of a risk-assessment scan, comprising:
- a) computer code for selecting a plurality of risk-assessment modules for execution during a risk-assessment scan, the risk-assessment modules each including vulnerability checks, and requiring communication via at least one predetermined port;
  - b) computer code for determining a set of ports for communicating with network components;
  - c) computer code for executing a port scan of the set of ports associated with the selected risk-assessment modules and the network components, for reducing the number of ports scanned during the port scan, wherein latency is reduced since a port scan involving 65,536 ports is avoided;

-7-

- d) computer code for modifying the set of ports based on the port scan, the set of ports being modified to include only ports available for communicating with the network components;
- e) computer code for comparing the port associated with each selected risk-assessment module with the modified set of ports; and
- f) computer code for conditionally disabling the execution of the risk-assessment modules based on the comparison to minimize the duration of the risk-assessment scan.

24. (Cancelled)

25. (Previously Presented) The method as recited in claim 1, wherein the risk-assessment modules include a web server vulnerability module with a predetermined port of 80, an e-mail vulnerability module with a predetermined port of 31337, and a Trojan program vulnerability module with a predetermined port of 25.